
Microsoft
Azure Networking
한국마이크로소프트 구명근

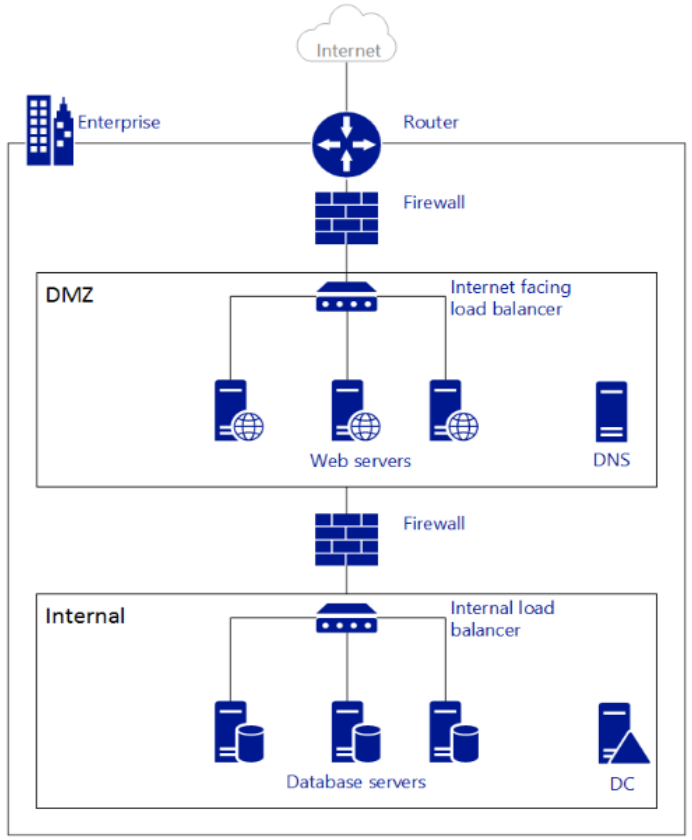
Agenda

- 가상 네트워크
- 가상 네트워크 연결
- 네트워킹 서비스

가상 네트워크

- 가상 네트워크는 온-프레미스의 네트워크를 Azure Cloud에서 논리적으로 정의한 네트워크 환경
- 하나의 가상 네트워크내에 IP 주소, DNS, 보안 그룹, 경로 테이블 제어 가능
- 가상 네트워크는 서브넷으로 세분화
- 다른 가상 네트워크 또는 온-프레미스의 네트워크에 연결 가능

가상 네트워크

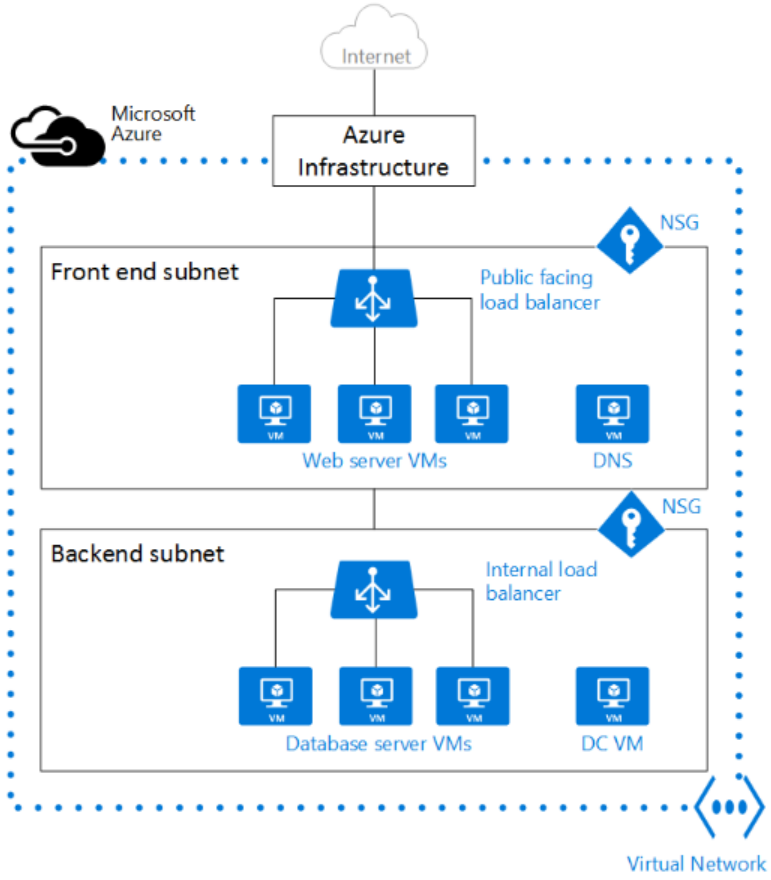


Router → 가상 네트워크 경로 테이블

Firewall → 네트워크 보안 그룹

DMZ, Internal → 서브넷

Load Balancer → SLB



가상 네트워크의 IP 주소와 이름 조회

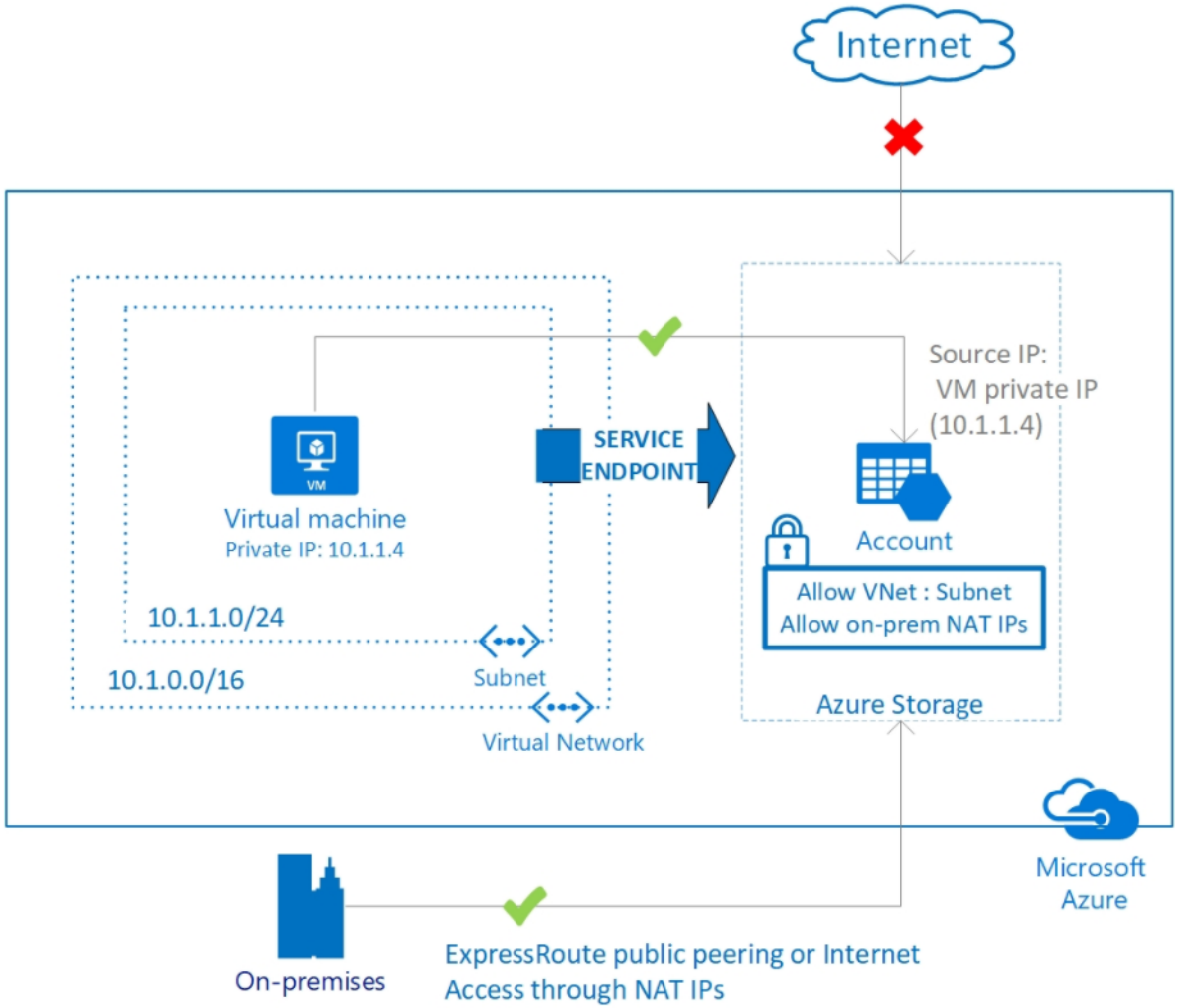
- 각 가상 머신은 개인 IP 주소를 부여 (Dynamic IP – DIP)
  - 생성시 부여받은 개인 IP 주소는 제거시까지 변경되지 않음
  - DNS Sever등과 같이 고정 개인 IP 주소가 필요할 경우 포털 또는 PowerShell로 설정 가능
- *.internal.cloudapp.net 는 내부 DNS(iDNS)를 통하여 개인 IP 주소로 변환

```
[azureuser@VM-LINUX-TEST ~]$ cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search xo21vwsv1luupngzmjzzc1sfsc.syx.internal.cloudapp.net
nameserver 168.63.129.16
```

- 별도의 DNS Server를 사용하면 DNS 접미사는 미제공
- iDNS는 동일한 가상 네트워크 내에 있는 가상 머신에 대해서만 조회가 가능

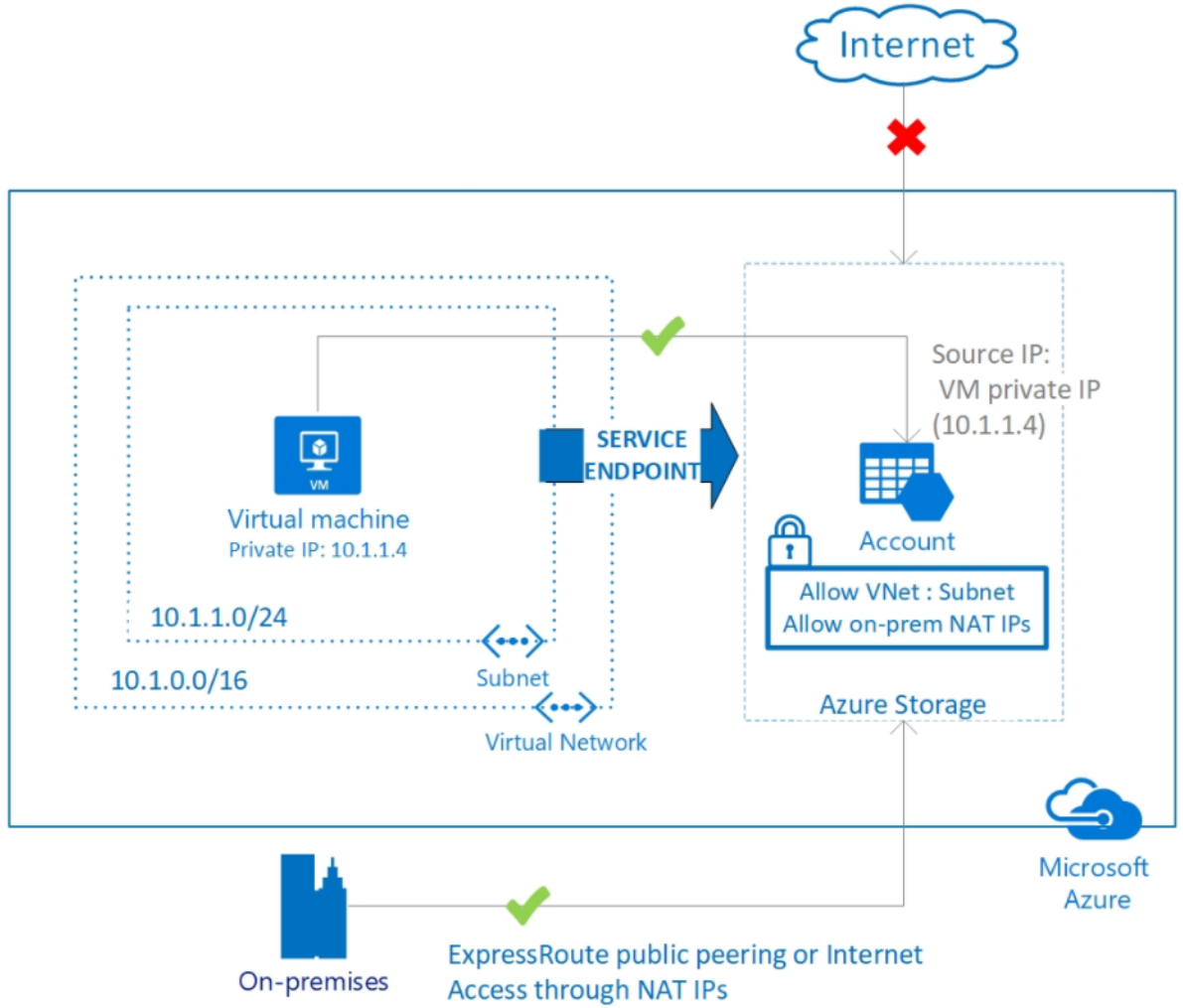
가상 네트워크 서비스 엔드포인트

- 가상 네트워크 주소 공간을 확장
- 온-프레미스에서 서비스 엔드포인트로 연결은 공용 인터넷을 통하여 접근하거나, 전용선(ExpressRoute)를 통하여 사용 가능 (단, 온-프레미스 장비는 공용 IP 주소가 필수)

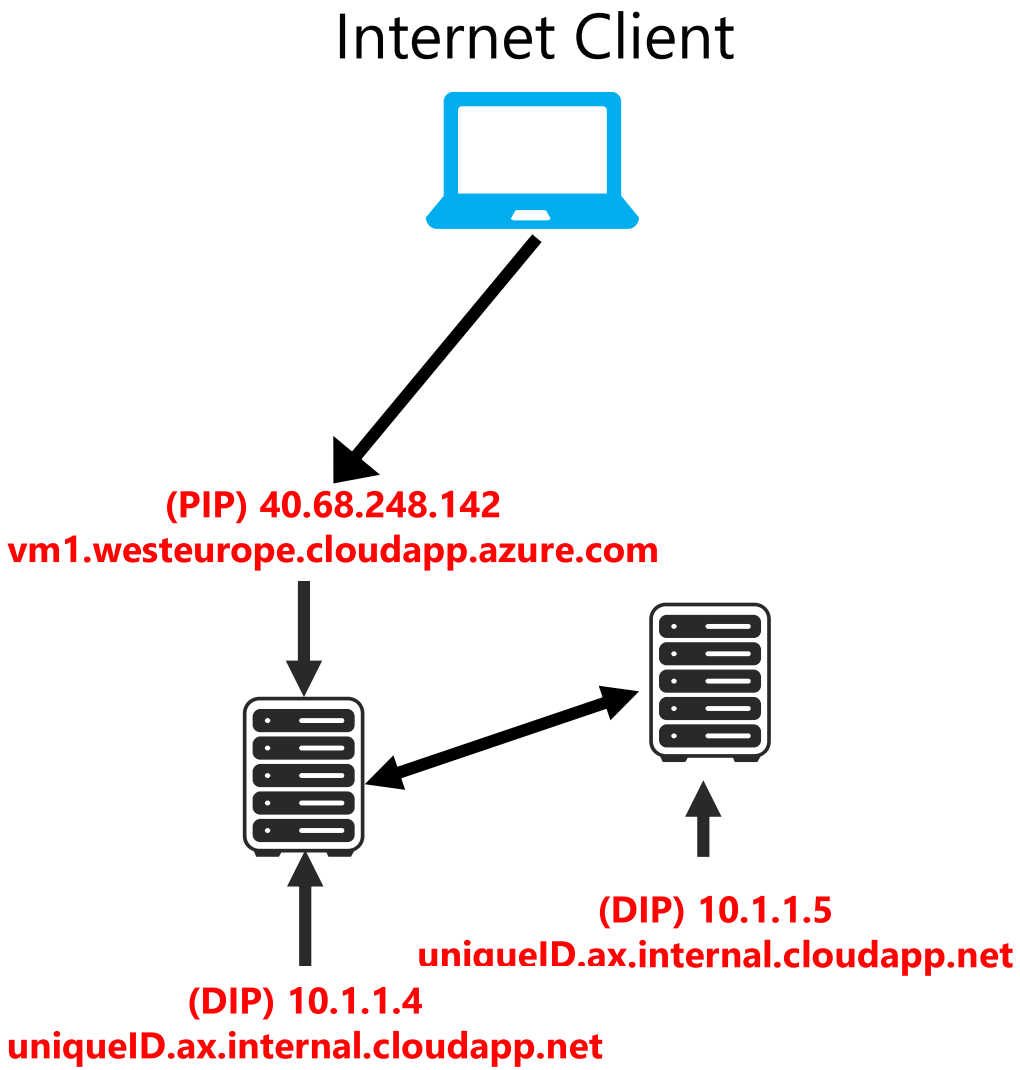


가상 네트워크 서비스 엔드포인트

- **사용 가능**
  - Azure Storage
  - Azure SQL Database
  - Azure Database for PostgreSQL
  - Azure Cosmos DB
  - Azure Key Vault
- **미리보기**
  - Azure SQL Data Warehouse
  - Azure Service Bus
  - Azure Event Hub
  - Azure Data Lake Store Gen 1

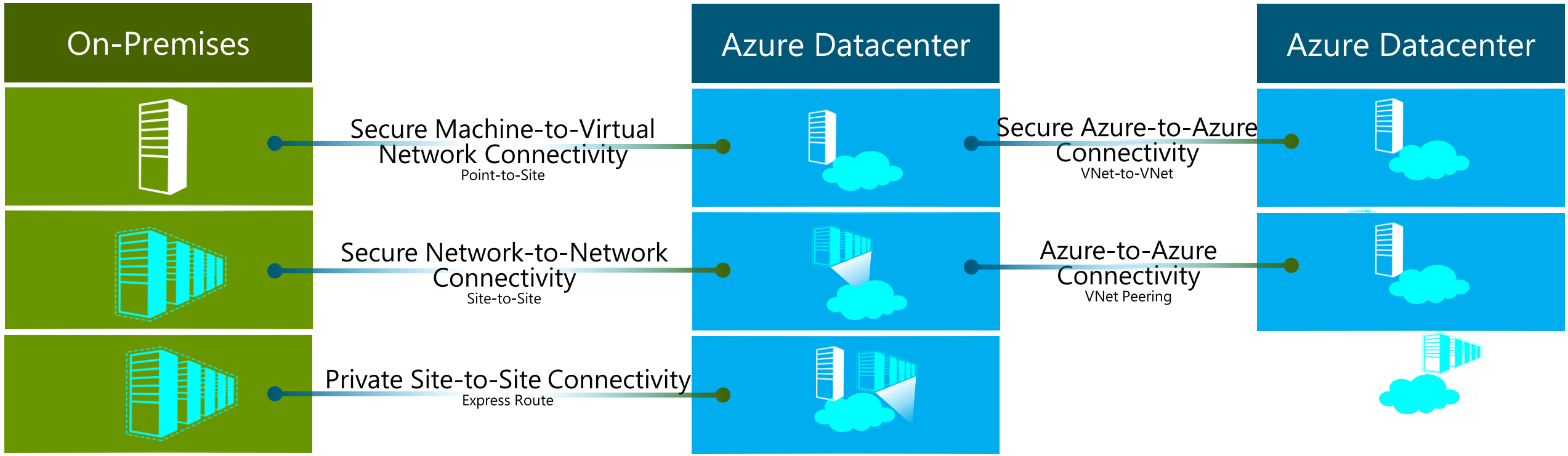


가상 네트워크 연결



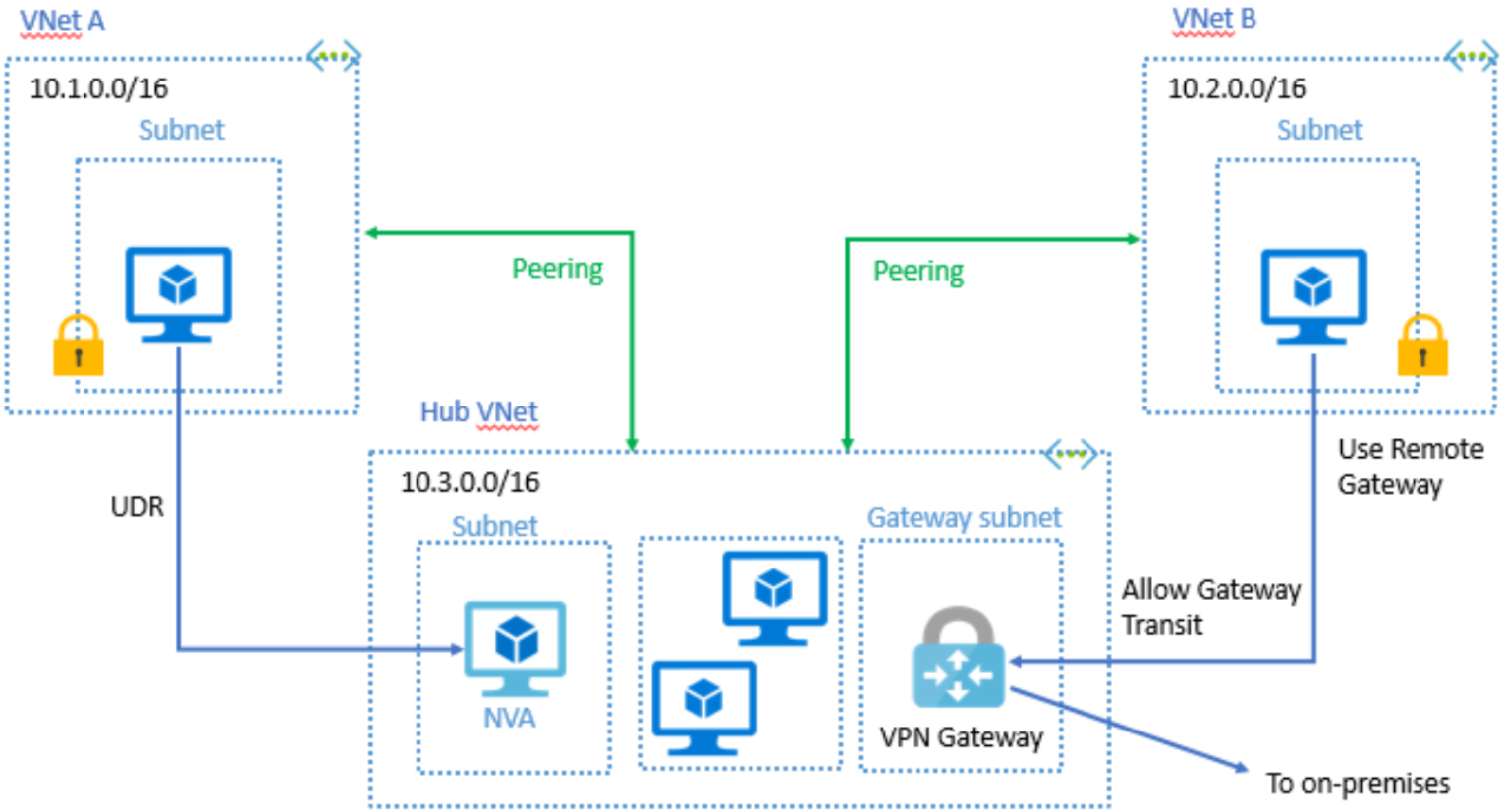
- 공용 IP 주소 (Public IP - PIP)
  - 가상머신 NIC의 DIP와 바인딩되며 인터넷을 통해 가상머신과 통신 가능
  - 각 NIC는 별도의 공용 IP주소를 예약 가능
  - Azure DNS서버의 cloudapp.azure.com zone의 A Record에 할당
- 동적 IP 주소 (Dynamic IP - DIP)
  - 각 NIC는 별도의 개인 IP 주소를 예약
  - 자동 생성된 고유 호스트 이름을 가진 DNS A Record에 할당
  - Azure iDNS 서버의 ax.internal.cloudapp.net zone에 저장

가상 네트워크 연결 – 옵션


On-Premises
Azure Datacenter
Azure Datacenter
Secure Machine-to-Virtual Network Connectivity
Point-to-Site
Secure Network-to-Network Connectivity
Site-to-Site
Private Site-to-Site Connectivity
Express Route
Secure Azure-to-Azure Connectivity
VNet-to-VNet
Azure-to-Azure Connectivity
VNet Peering

가상 네트워크 연결 – Peering

- Microsoft의 백본 인프라를 통하여 Azure 가상 네트워크를 다른 가상 네트워크와 확장



가상 네트워크 연결 – Peering

- 가상 네트워크를 게이트웨이없이 두 네트워크간에 연결성 제공
- 동일 또는 다른 지역(Region)의 2개의 가상 네트워크 연결
- 두 네트워크가 하나의 연결로 표시되지만 별도의 리소스로 관리
- 중첩된 IP 주소 범위 지원 불가
- 가상 네트워크와 리소스 사이에 낮은 지연시간, 높은 대역폭
- 송수신 트래픽 데이터 전송 요금 청구
- 라우팅 프로토콜 미지원 – Transitive 라우팅 관계 성립 불가
  - A ↔ B, B ↔ C일 경우, A ↔ C는 연결되지 않음

가상 네트워크 연결 – VPN 게이트웨이

- 네트워크를 통해 다른 네트워크 엔드 포인트로 트래픽을 송수신하는 가상 네트워크 게이트웨이
- 가상 네트워크별로 하나의 VPN 게이트웨이가 할당
- 암호화된 트래픽

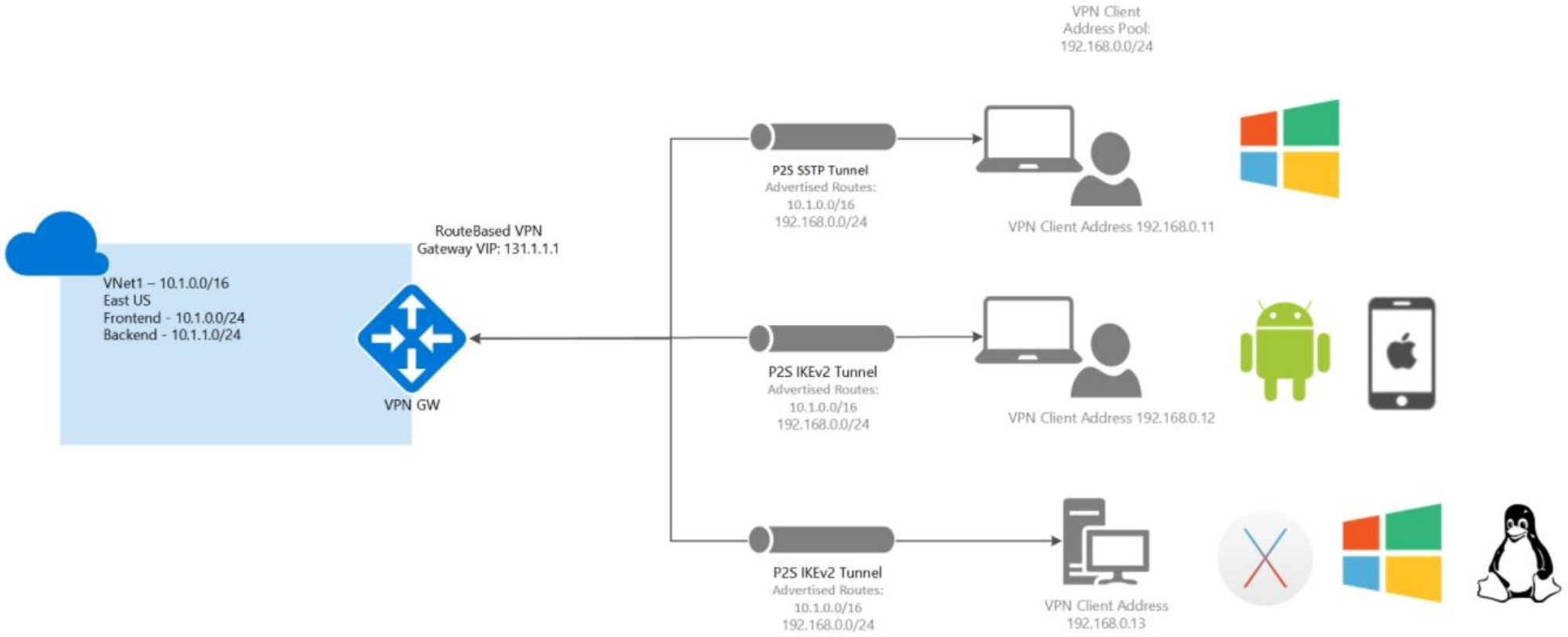
SKU	S2S/VNet 간 터널	P2S SSTP 연결	P2S IKEv2 연결	집계 처리량 벤치마크	BGP
Basic	최대 10	최대 128	지원되지 않음	100Mbps	지원되지 않음
VpnGw1	최대 30*	최대 128	최대 250	650Mbps	지원됨
VpnGw2	최대 30*	최대 128	최대 500	1Gbps	지원됨
VpnGw3	최대 30*	최대 128	최대 1000	1.25Gbps	지원됨

가상 네트워크 연결 – VPN 게이트웨이 종류

- 경로 기반 VPN 게이트웨이
  - any-to-any(와일드카드) 트래픽 선택기를 사용
  - BGP, 강제 터널링 및 다중 사이트 VPN 터널 지원
- 정책 기반 VPN 게이트웨이
  - IPSec 터널을 통해 트래픽이 암호화/복호화되는 방식을 정의하기 위해 두 네트워크 접두사의 조합을 사용
  - 패킷 필터링을 수행하는 방화벽 장치 기반
  - BGP, 강제 터널링 및 다중 사이트 VPN 터널 미지원

가상 네트워크 연결 – P2S

- Point-to-Site(P2S) 연결
  - SSTP 또는 IKEv2 터널을 사용하여 Azure 가상 네트워크를 단일 또는 여러 컴퓨터로 확장



https://docs.microsoft.com/ko-kr/azure/vpn-gateway/point-to-site-about

가상 네트워크 연결 – P2S

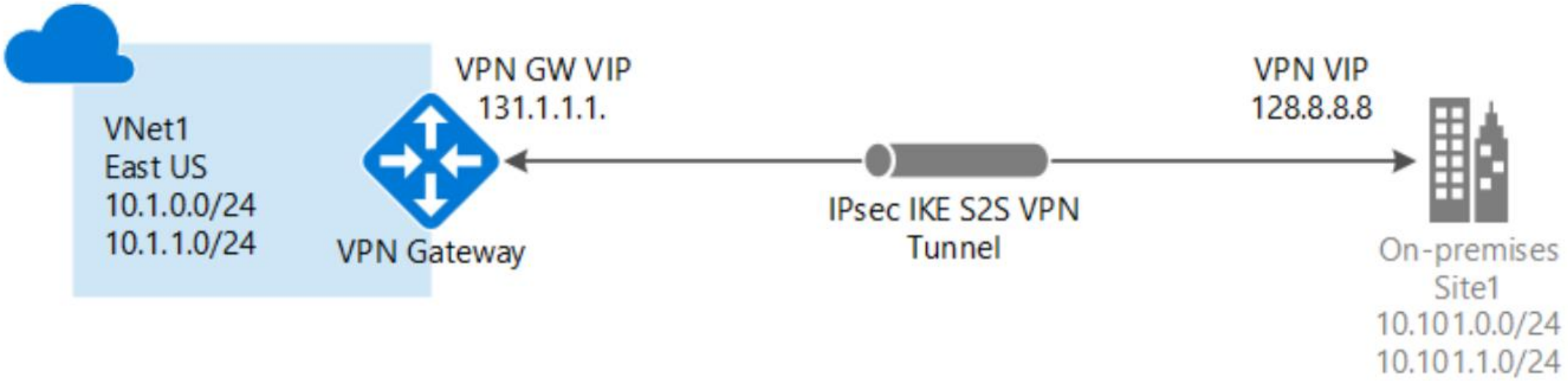
- 가상 네트워크 게이트웨이에 대한 VPN 클라이언트 연결을 기반
- Azure 또는 고객이 제공한 인증서, Azure AD(Active Directory) 또는 RADIUS인증을 사용하여 VPN 클라이언트를 인증
- 인터넷을 통하여 SSTP(Secure Socket Tunneling Protocol) 및 IKEv2(IPSec) VPN Tunnel을 지원
- Windows 7, Mac OSX 10.11 이상 및 IKEv2를 지원하는 Linux를 지원
- SSTP 연결은 최대 128개의 VPN 클라이언트 연결을 지원

SKU	S2S/VNet 간 터널	P2S SSTP 연결	P2S IKEv2 연결	집계 처리량 벤치마크
VpnGw1	최대 30	최대 128	최대 250	650Mbps
VpnGw2	최대 30	최대 128	최대 500	1Gbps
VpnGw3	최대 30	최대 128	최대 1000	1.25Gbps
Basic	최대 10	최대 128	지원되지 않음	100Mbps

https://docs.microsoft.com/ko-kr/azure/vpn-gateway/point-to-site-about

가상 네트워크 연결 – S2S

- Site-to-Site(S2S) 연결
  - 인터넷을 통해 IPSec/IKEv2 VPN Tunnel을 사용하여 온-프레미스 네트워크를 Azure 가상 네트워크로 안전하게 확장



https://docs.microsoft.com/ko-kr/azure/vpn-gateway/point-to-site-about

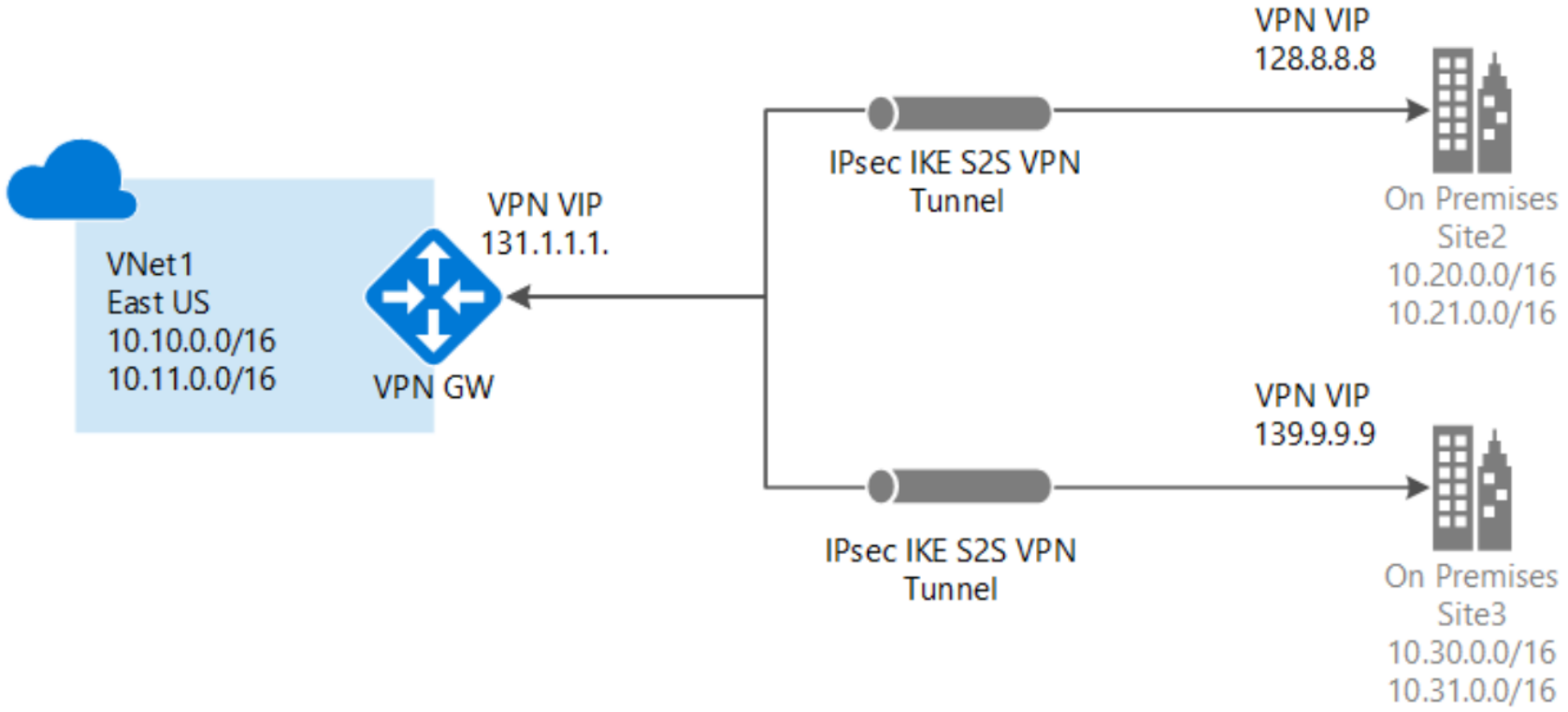
가상 네트워크 연결 – S2S

- IPSec/IKE(IKEv1 또는 IKEv2) VPN Tunnel을 사용하여 두 네트워크간 연결을 제공
- 로컬 네트워크 게이트웨이 필요
- 게이트웨이 사이에 인증을 위하여 사전 공유 Key 사용
- BGP 및 강제 터널링 지원
- 활성-활성 모드 지원
- 온-프레미스와 Azure 가상 네트워크 사이에 IP 주소 범위가 중첩 불가
- 구성이 되면 Azure 가상 네트워크에서 온-프레미스 내 솔루션을 사용 가능

  ex) 도메인 컨트롤러, 모니터링, 백업 툴, 기타..

가상 네트워크 연결 Multi-Site VPN

- Multi-Site VPN 연결
  - 여러 지점의 사이트를 단일 가상 네트워크 게이트웨이에 연결

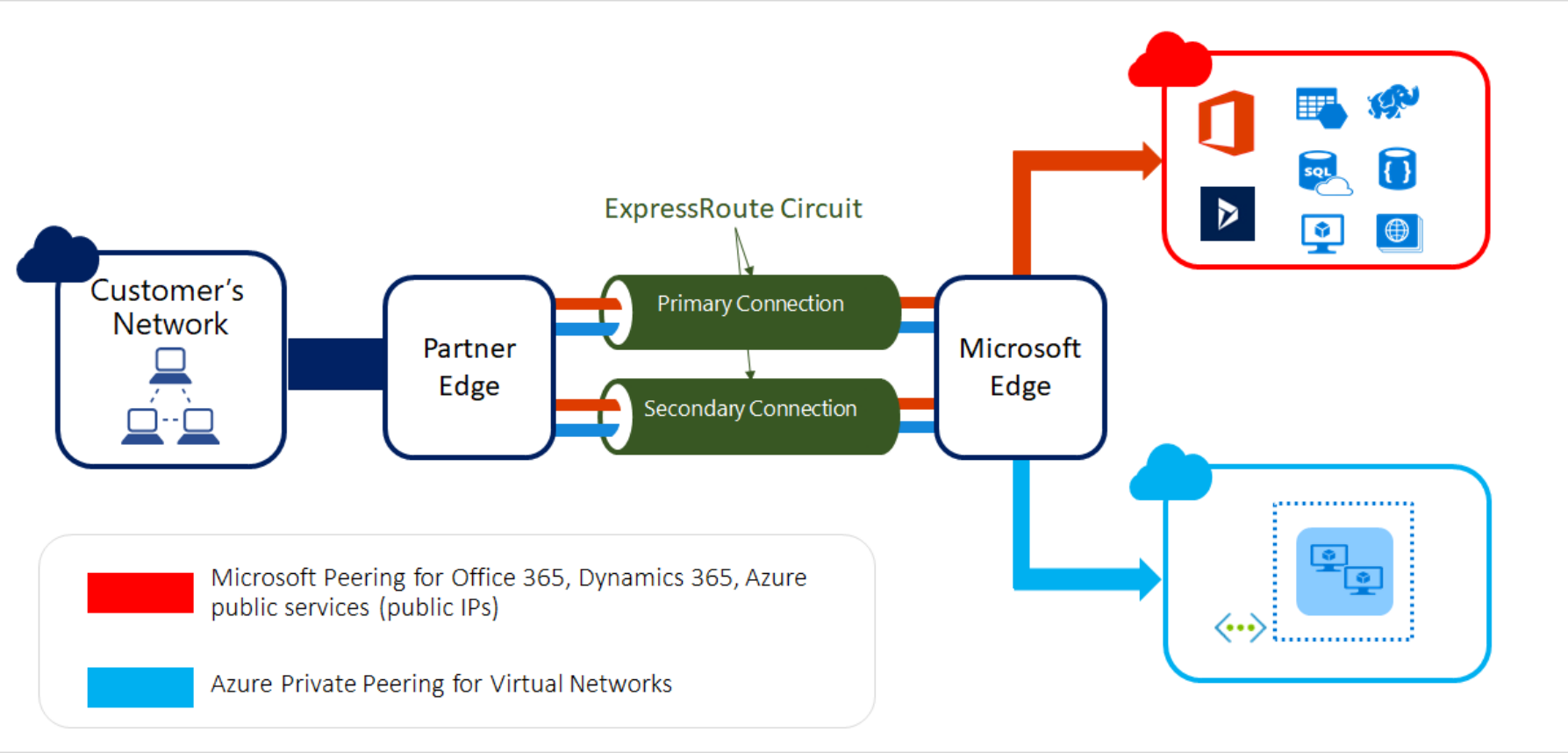


가상 네트워크 연결 Multi-Site VPN

- 온-프레미스 VPN 게이트웨이가 경로 기반 VPN을 지원하는지 확인 필요
- 겹치는 IP 주소 범위는 지원 불가

가상 네트워크 연결 – ExpressRoute

- 전용선을 사용하여 온-프레미스와 Azure Cloud를 연결

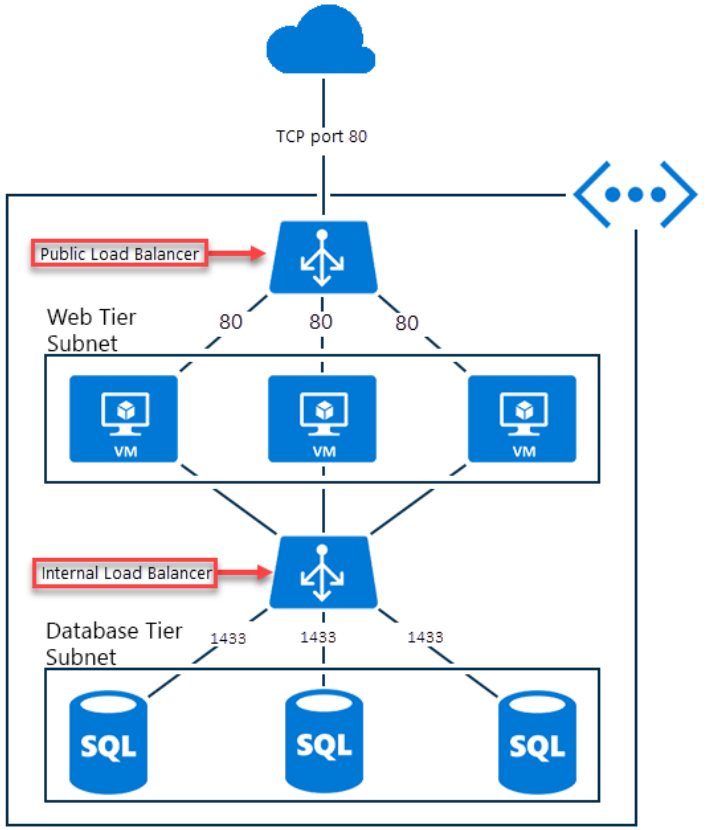


가상 네트워크 연결 – ExpressRoute

- 고가용성을 위한 중복 연결 제공
  - 활설-활성 를 기본으로 두개의 독립 BGP 세션으로 중복 구성
- Private Peering과 Microsoft Peering 지원
  - Private Peering은 Azure 가상 네트워크와 온-프레미스 사이에 RFC 1918표준을 준수
  - Microsoft Peering은 Office 365, Dynamics 365, Azure PaaS 서비스간에 연결
- 데이터 암호화는 기본적으로 포함되어 있지 않으며, 공급자 또는 고객이 구현
- 하나의 ExpressRoute 연결을 구독간에 공유해서 사용 가능

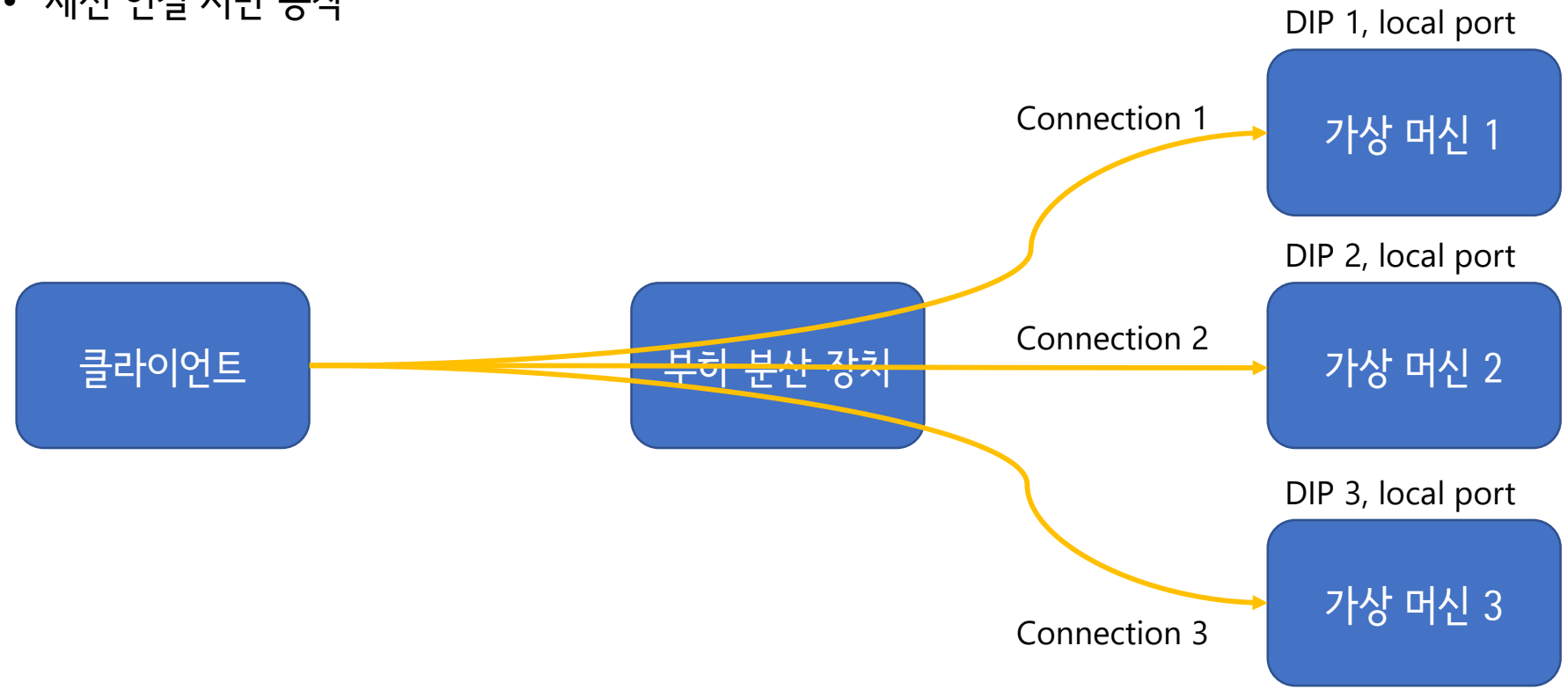
네트워크 서비스 – 부하 분산 장치

- 들어오는 트래픽을 정의된 서비스 인스턴스간에 분산(TCP/UDP)
- 유형
  - 공용 부하 분산 장치
  - 내부 부하 분산 장치
- 기능
  - 부하 분산
  - 포트 전달
  - 자동 재구성
  - 상태 프로브
  - 아웃바운드 연결(SNAT)



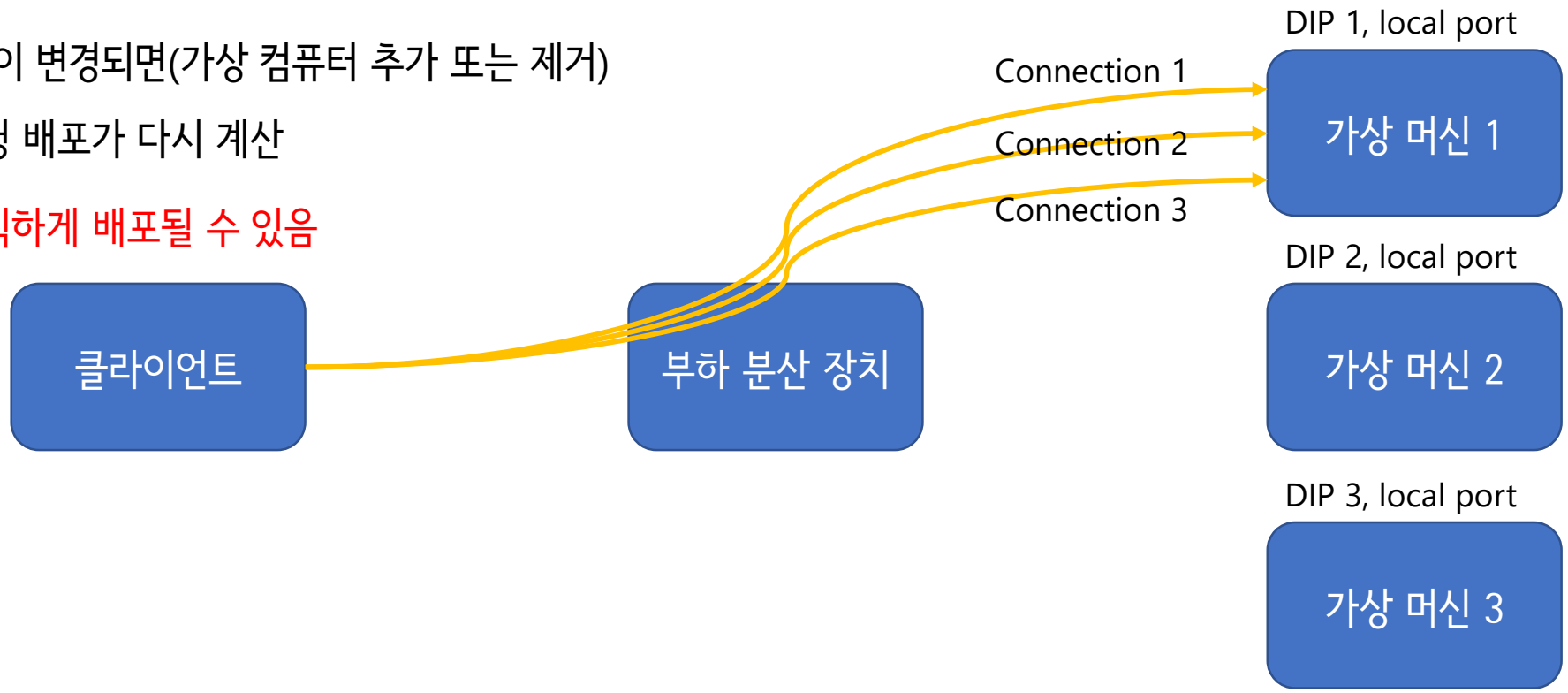
네트워크 서비스 – 부하 분산 장치

- 해시 기반 배포 모드
  - 5개 튜플(원본 IP, 원본 포트, 대상 IP, 대상 포트, 프로토콜 종류)
  - 세션 연결 시만 동작



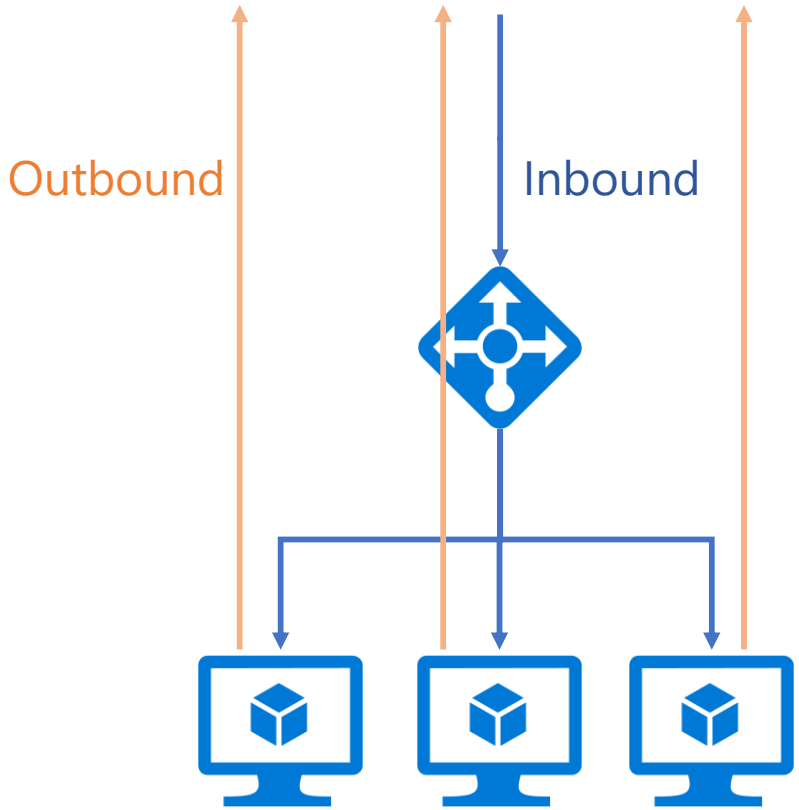
네트워크 서비스 – 부하 분산 장치

- 소스 IP 선호도 모드
  - 2개 튜플(원본 IP, 원본 포트)
  - 3개 튜플(원본 IP, 대상 IP, 프로토콜)
  - 부하 분산 집합이 변경되면(가상 컴퓨터 추가 또는 제거) 클라이언트 요청 배포가 다시 계산
  - 트래픽이 불규칙하게 배포될 수 있음

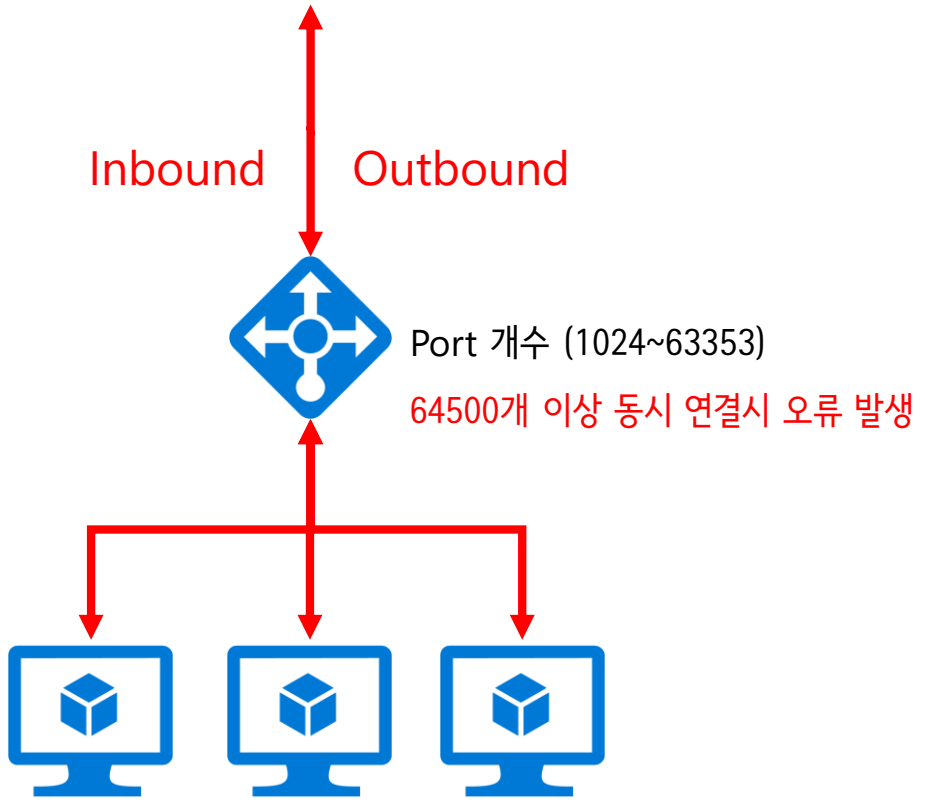


네트워크 서비스 – 부하 분산 장치

- 부하 분산 장치의 아웃바운드 연결



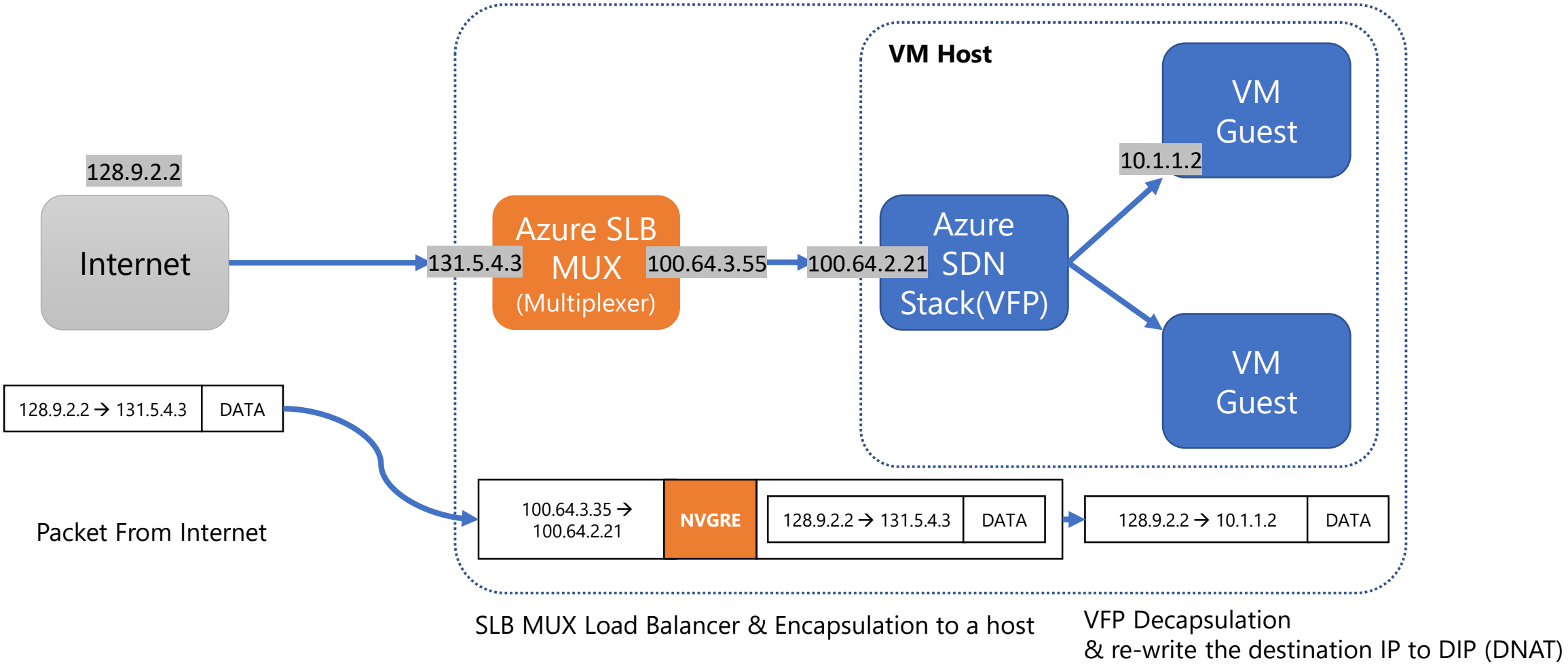
- 가상 머신에 공인 IP주소가 있음
- 부하 분산장치의 SNAT 미사용



- 가상 머신에 공인 IP주소가 있음 (또는 없음)
- 부하 분산장치의 SNAT 을 사용

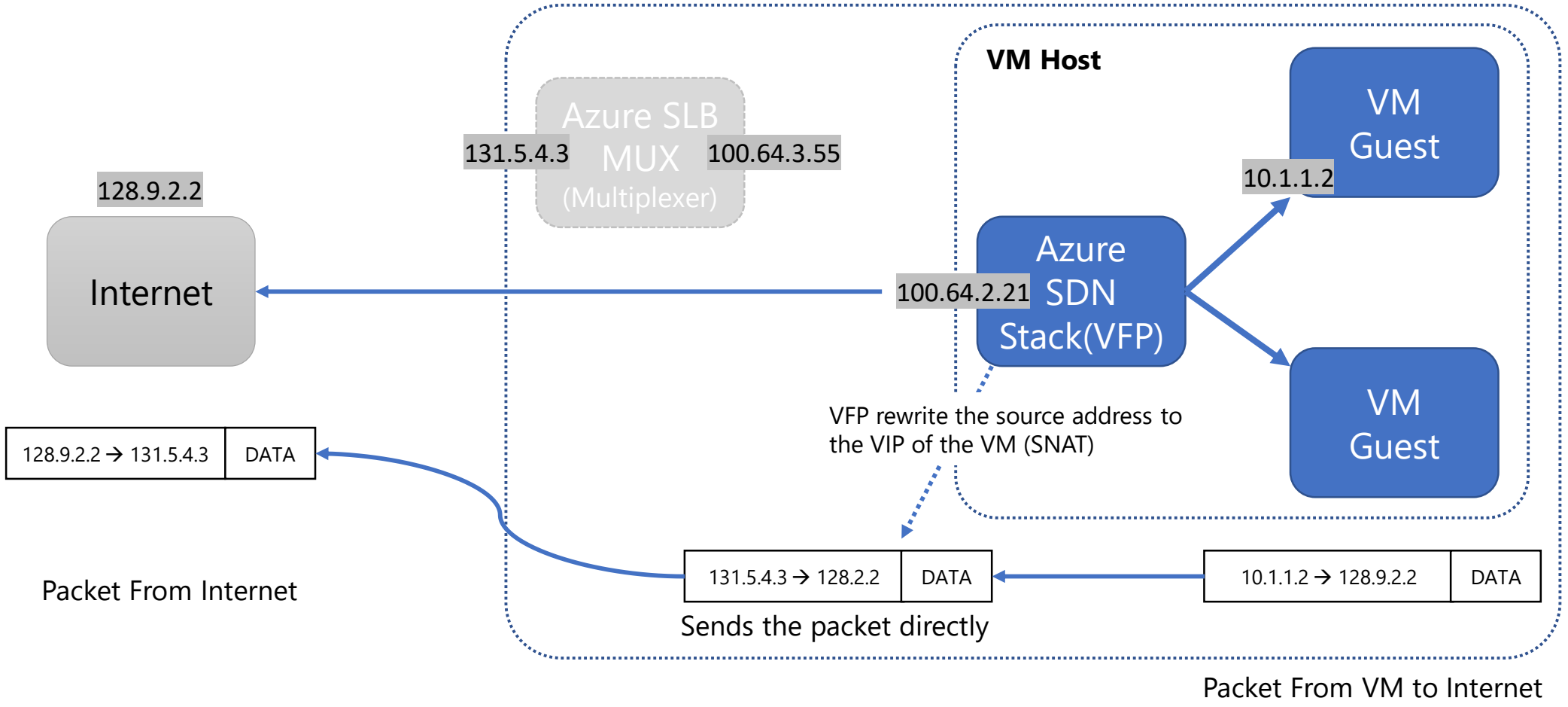
네트워크 서비스 – 부하 분산 장치

- SLB DNAT



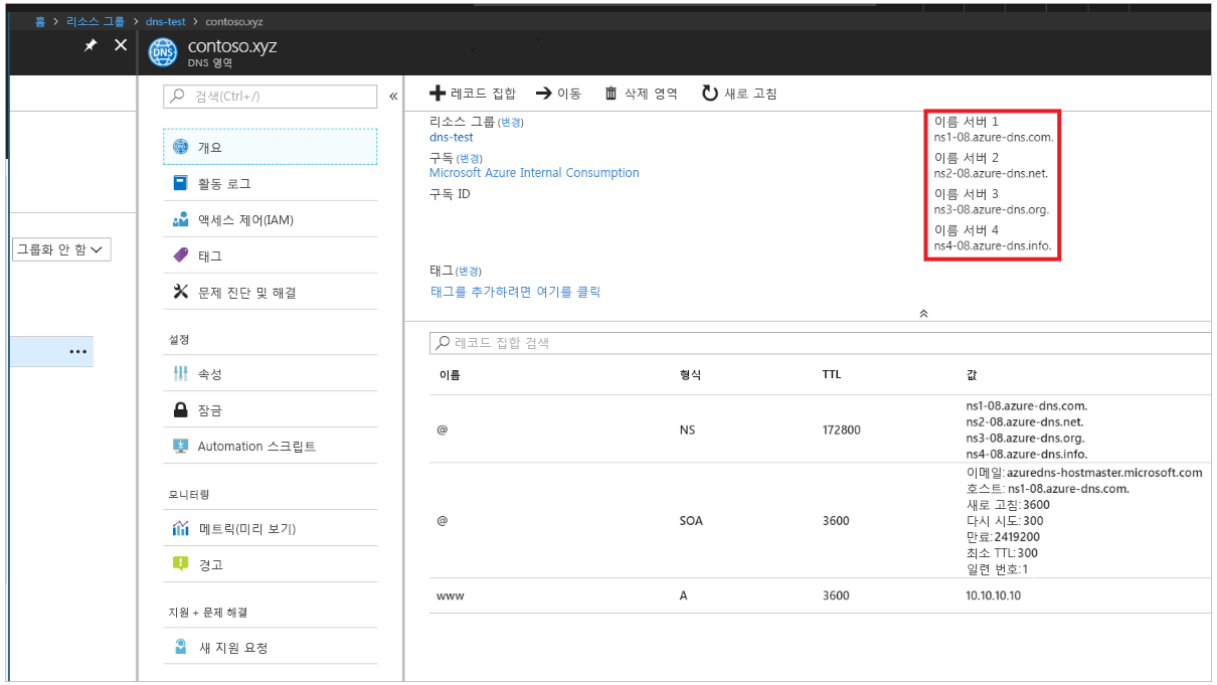
네트워크 서비스 – 부하 분산 장치

- SLB SNAT



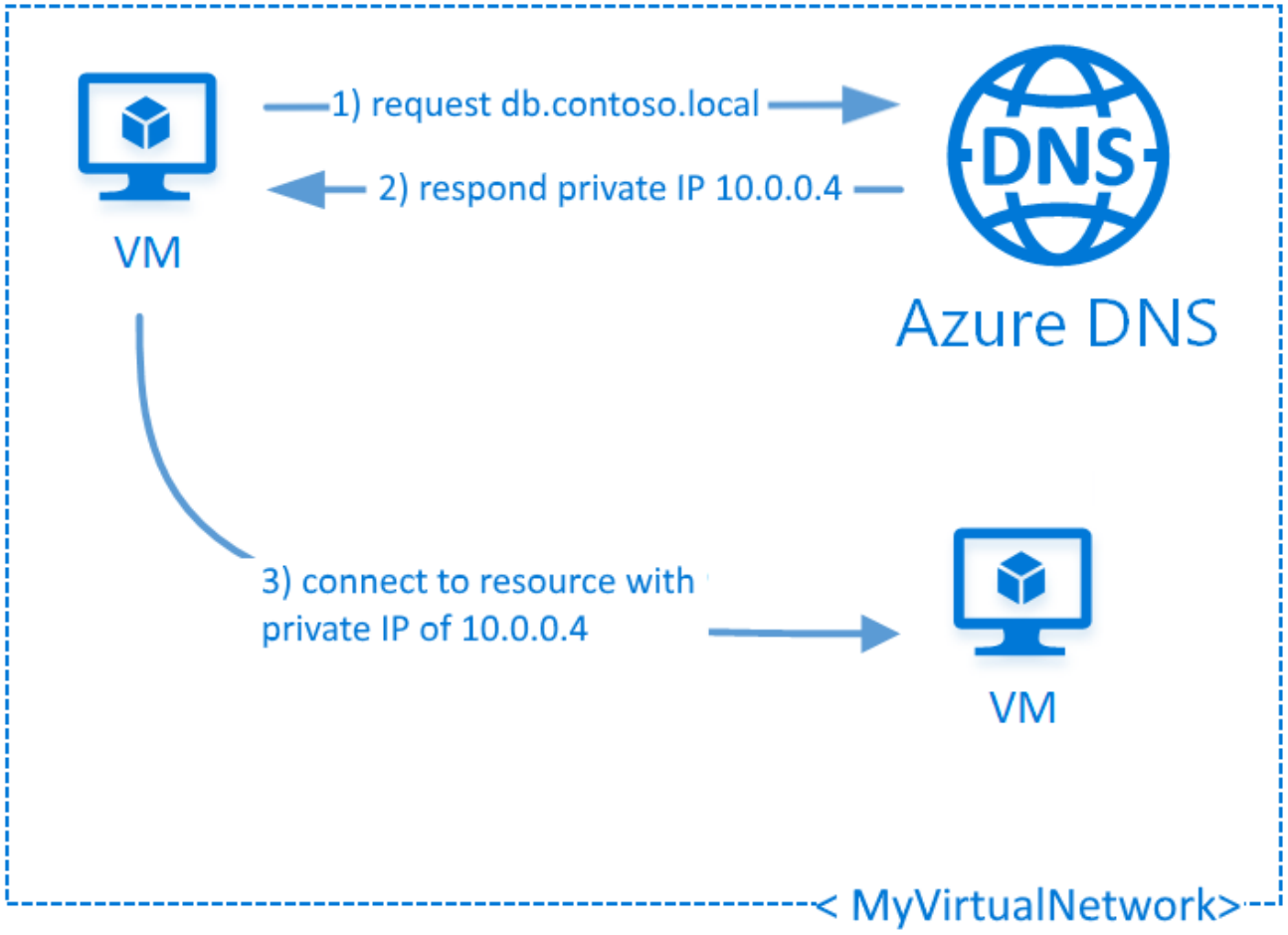
네트워크 서비스 – DNS 영역

- 도메인 호스팅
- DNS 레코드 관리
- 레코드 형식
  - A, AAAA, CNAME, MX, NS, PTR, SOA, SRV, TXT
- 별칭 레코드 집합을 지원
- 와일드카드 레코드 지원
- 영역당 레코드는 5000개까지 지원



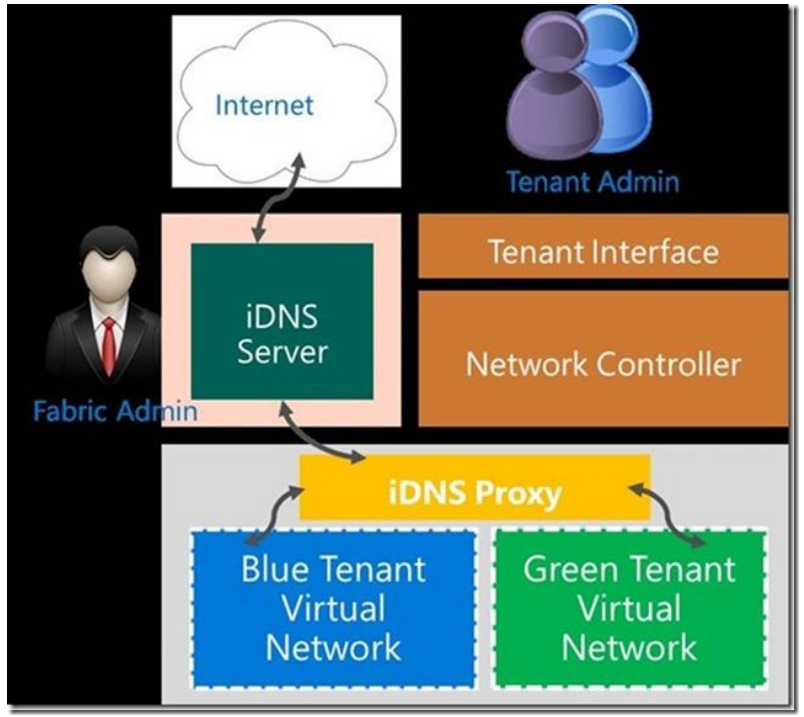
네트워크 서비스 – 사설 DNS 영역 [미리보기]

- 사용자 지정 도메인 솔루션을 사용하지 않고도 가상 네트워크 내의 도메인을 관리
- 모든 공용 DNS 레코드 형식 지원
- 자동 호스트 레코드 관리
- 비어 있는 가상 네트워크에 PowerShell로 생성 (미리보기)



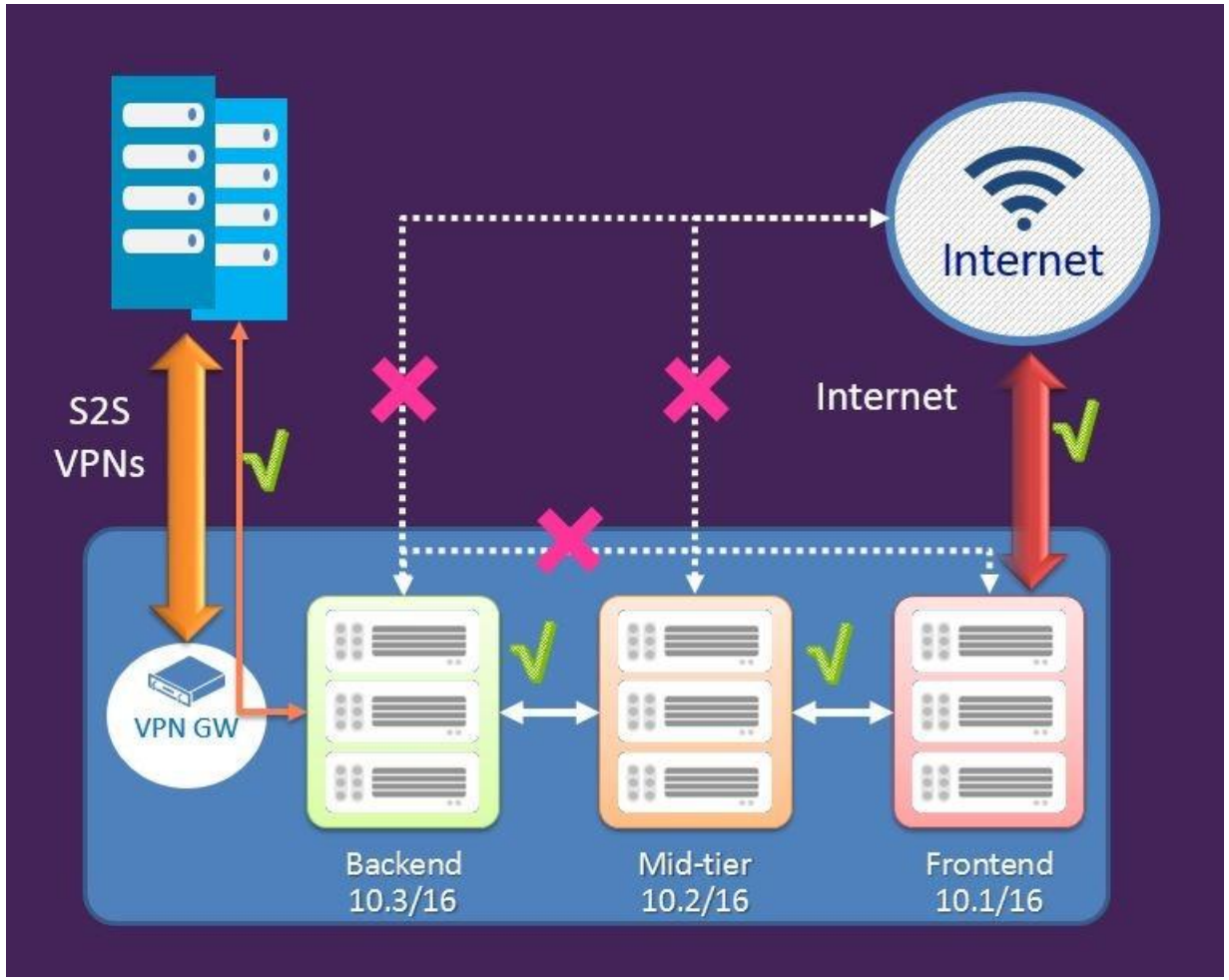
네트워크 서비스 – DNS 서비스

- iDNS (Internal DNS) Proxy
- 어떤 VM을 만들어도 내부 DNS 주소는 168.63.129.16
- VM으로 부터 DNS 조회 요청을 Hyper-V가 받아서 DNS가 준 것처럼 반환
- 네트워크 보안 그룹에서 168.63.129.16을 막으면 문제 발생
  - DNS Lookup이 불가능
  - Agent도 이 IP로 통신



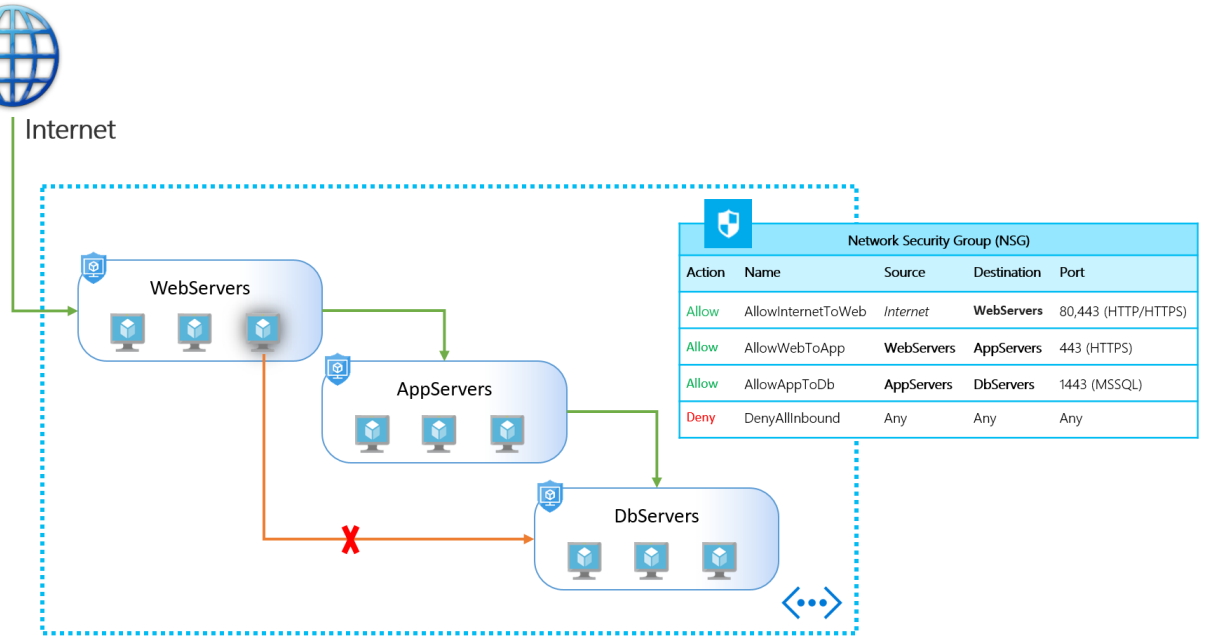
네트워크 서비스 – 네트워크 보안 그룹(NSGs)

- 서브넷의 VM / NIC 또는 가상머신 그룹에 대한 송수신 트래픽에 대한 접근 제어 규칙을 정의
- 규칙은 우선 순위에 따라 처리
- 이중 보안으로 잡아도 Rule/Flow Table을 참조하여 네트워크에서 계산하여 위에서 버림
- 방화벽 대체



네트워크 서비스 – 응용프로그램 보안 그룹(ASGs)

- 가상 머신에서 실행되는 응용 프로그램을 그룹화 하여 보안을 관리
- 네트워크 보안 그룹을 응용 프로그램을 중심으로 사용
- 네트워크 보안그룹은 IP 주소로 관리되기때문에 대상의 IP 주소가 변경되면 규칙이 변경해야하는 복잡성을 우회



네트워크 서비스 – DDOS 보호

- 실제 네트워크 트래픽을 모니터링 하고 DDoS 정책에 정의 된 임계 값과 지속적으로 비교
- 트래픽 임계 값을 초과하면 DDoS 완화가 자동으로 시작
- 검사 수행
  - 패킷 형식(인터넷 사양) 준수 및 잘못되었는지 확인
  - 스프핑 된 패킷 확인 (SYN Auth, SYN Cookie 또는 원본을 위해 패킷을 삭제 하고 재전송)
  - 다른 통신을 수행할 수 없을 정도의 속도 제한 패킷
- DDoS 보호 모드
  - Basic
  - Standard

Microsoft

감사합니다